(4)

e-Sign: Online Digital Signature Service using Aadhaar

Authors: Dr. Pramod K Varma and Sasikumar Ganesan

**** e-Sign is a temporary name given to the proposed scheme to make reading of rest of the document easier.***

Introduction

Currently personal digital signature requires person's identity verification and issuance of USB dongle having private key, secured with a password/pin. As per IT Act, DSC private key must be stored using secure storage devices like USB tokens, smart cards, etc. This is achieved via issuance of physical tokens and identity verification is done by validating against an identity document. For class III, physical presence of the individual is also required.

Scaling DSC Usage

Current scheme of physical verification, document based identity validation, and issuance of physical dongles does not scale to a billion people. Current scheme requires issuance of millions of USB dongles, people to keep track of the token and passwords, etc. For mass adoption of DSC, a simple online service must be designed that allows anyone in this country to have the ability to sign a document with no complexity.

**** Note: Authors are NOT proposing replacement of current scheme, rather, an addition of an online alternative for mass adoption of DSC.***

This document proposes a solution, in addition to current scheme, via an online service using Aadhaar e-KYC allowing any Aadhaar holder (currently 630+ million people) to sign any document with just Aadhaar biometric/OTP authentication requiring no physical dongle issuance and management!!

For lack of name, henceforth in this document, this online service specification will be referred as "***e-Sign***" service.

Concept at High Level

e-Sign service provides a scheme by which any Aadhaar holder can digitally sign any document using an online service. This service authenticates the person, does Aadhaar e-kyc, and then digitally signs the input within the e-Sign provider backend. Such scheme allows DSC to be scaled massively and allow many 3rd party applications to use the service via an open API and integrate DSC into their application.

A specification ("***e-Sign Technology and API Specification***") should provide a standardized API and technology details for such a service. It is proposed that CCA puts out this specification and allow multiple approved/empanelled providers to offer e-Sign service compliant to this specification. Such multi-provider system ensures healthy competition from the point of view of service quality, uptime, price, reporting, etc.

At a high level, applications needing to sign any document do the following:

1. 3rd party application asks the end user for the document to sign
2. Creates the document hash (to be signed) on the client side
3. Capture Aadhaar number and authentication factor
    a. For class II, use any of biometric/OTP
    b. For class III, use biometric
4. Creates the e-Sign API input
5. Calls the e-Sign API of their preferred provider
6. Provider validates the calling application, input, and then creates the Aadhaar e-KYC input based on Aadhaar e-KYC API specification
7. e-Sign Provider (a KUA as per Aadhaar e-KYC model) invokes the Aadhaar e-KYC API
8. On success, e-Sign provider creates a new key pair for that Aadhaar holder
9. Signs the input document hash using the private key(Note: The original document never leaves the actual computer)
10. e-Sign provider creates an audit for the transaction
    a. Audit includes the transaction details, timestamp, and Aadhaar e-KYC response
    b. This is used for pricing and reporting
11. Sends the e-SIgn API response back to the calling application
12. 3rd party calling application attaches the signature to the document

e-Sign Service Providers

e-sign service can be provided by multiple providers approved by CCA. Every one of these service providers must comply to "***e-Sign Technology and API Specifications***". Compliance can be done via testing and certification ("*e-Sign Certified*").

This ensures that a multi provider ecosystem is created allowing healthy competition for such a service. Authors recommend that **at least** all approved CAs should be allowed to create and host such a service and the sub-CA's can use the same infrastructure of the CA to deliver service. We also suggest 3rd party organizations (NIUs and private) may be allowed to offer such an online service as long as they are "certified for compliance" and empanelled. These service providers can price the e-Sign service and pricing should be left to market forces.

It should be mandated that the keys be stored in the secured device like HSM or key managers and strict standards similar to FIPS 140-2 Level 3 be created and audited with open standards. The entire certification and compliance audit mechanism could also be implemented through partners/consortium.

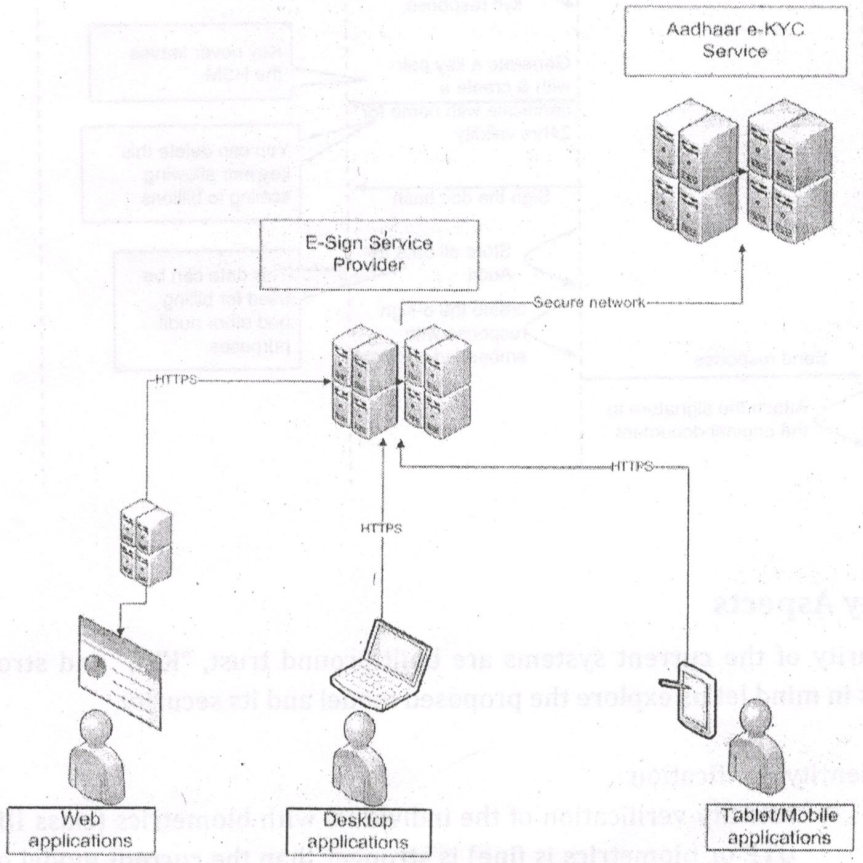
Possible Applications

E-sign service can be used for the following means.

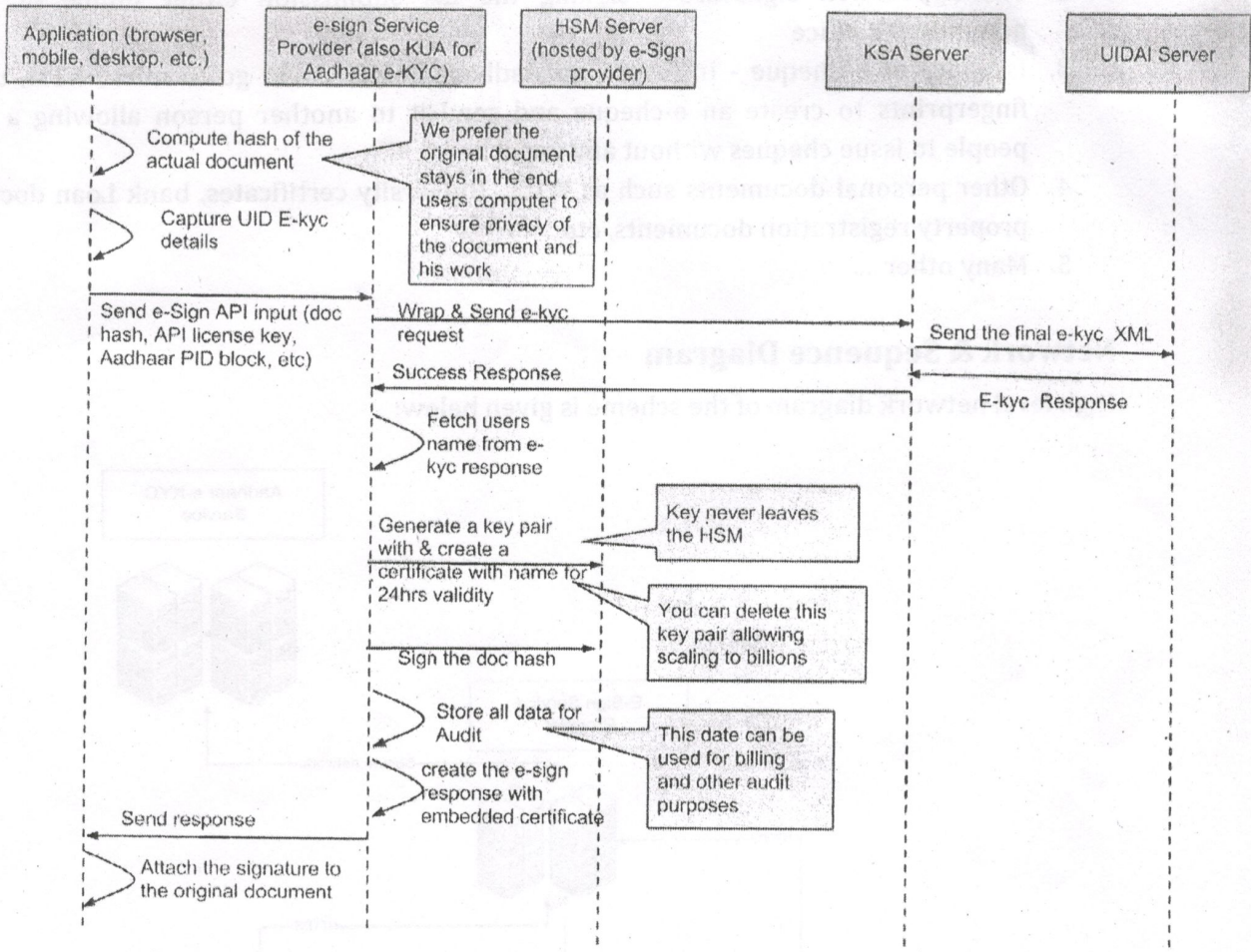
1. Government document signatures - integrating this to Govt e-file and workflow application for signing the documents.
2. Tax application signature - signing the tax submission either online or at the accountant's office
3. Issuance of e-Cheque - In future, an Aadhaar holder could go to micro-ATM, use her fingerprints to create an e-cheque and send it to another person allowing a billion people to issue cheques without any paper!
4. Other personal documents such as WILL, University certificates, bank Loan document, property registration documents, etc
5. Many other ....

Network & Sequence Diagram

High level network diagram of the scheme is given below:



API sequence diagram is given below:



Security Aspects

The security of the current systems are built around trust, "KYC" and strong crypto tokens. With this in mind let us explore the proposed model and its security.

- Identity Verification
  - Identity verification of the individual with biometrics (class III for class II either OTP or biometrics is fine) is stronger than the current model of document based verification
  - Name of the individual as in UIDAI database and online verifiable.
  - Verification and physical presence (for class III) is confirmed electronically and audit records are digitally signed and available for verification

- No compromisable/shareable passwords/PIN. Current model allows "proxies" to sign even when the owner is not available/alive!
- Using biometrics ensures only live people can sign the document!

- Storage
  - The signed document never leaves the end users computer (similar to the current USB model)
  - No storage of private keys anywhere in the entire eco system. Unlike USB dongles, this scheme does not allow "sharing" of keys for proxy signature.
  - Usage of HSM is compliant and compatible with secure storage requirement
  - Currently crypto tokens are shareable and in case of theft, it only has a 4 digit locally matched password to protect. e-Sign model has no shareable devices or passwords (secure and scalable).
- Key security and revocation
  - Keys are generated with 24hrs validity
  - No revocation or lost token issues
  - No storage of keys ensure less privacy and security incidents with reduction in customer support and maintenance.
  - The x509 format of the public key guarantees the issuer details and provides non-repudiation of key generation by third parties.
- Verification of signed document
  - Document verification process has no change.
  - Physical keys do not exist anywhere other than the signed document with x509 based public key.
  - Compatible with IT Act and secure crypto storage requirement of CCA
  - Verifiable anywhere and every document has different keys.
- Virus and Trojan attack in end user machine
  - Virus or Trojans cannot track or re-use OTP or biometrics when using registered devices.
  - As there is no PIN there is no chance of brute-force attacks or keyloggers tracking the pin entry from the user's host
  - No local OS dependency (no issues with drivers etc) since entire system resides on secure cloud of the s-Sign provider

e-Sign API at High Level

As part of e-Sign technology specifications, an open API should be defined to allow 3rd party applications needing to digitally sign a document to invoke the API. Any of the e-Sign service providers can expose this API via HTTPS. 3rd party applications (such as document workflow, tax filing, etc) can subscribe to the API with any of the service providers.

API Input

```
<esigni ts="" txn="" oid="" ak="">
      <input>document hash in hex</input>
      <auth>aadhaar auth XML without LK and DSC</auth>
</esigni>
```

ts: Request timestamp in ISO format

txn: Transaction ID of the 3rd party app calling the API, this is returned in the output for correlation

oid: ID of the organization subscribing to e-SIgn service. Billing/auditing is done against this organization.

ak: API access key to authenticate 3rd party calling apps. This should be

```
SHA-1(API_license_key + ts)
```

API license key can be issued by service providers to their API subscribers. This allows calling apps to be authenticated by the service provider and also have the billing/auditing to be tracked against the organization for which the license key is issued.

API Output

```
<esigno ts="" txn="" code="" err="">
      <signature>base-64 encoded signed hash XML with x509 certificate embedded</signature>
</esigno>
```

ts: Response timestamp in ISO format

txn: Transaction ID as it was in the input XML

code: A globally unique API response code in the form of UUID. e-Sign provider should maintain audits in their system against this unique API response code.

err: Error code if any. Specification should define a set of standard error codes so that applications moving from one provide to another do not need to change their application code.

Audit, Billing, and Reporting

e-Sign providers must maintain proper audits for all transactions. Based on their pricing structure, they can create billing and reporting modules and provide value added services to their subscribers.

Audit should contain the following elements:

- From main input XML - "ts", "txn", "oid"
- From within "Auth" element of input - "uid", "tid", "txn"
- From output - "ts", "code", "err"
- Decrypted Aadhaar eKYC response

Other notes on audit:

- Aadhaar KUA audit compliance is required by the e-Sign provider
- e-Sign provider should ensure audit records are signed to ensure no tampering is possible. It is recommended that provider create an audit XML containing all elements, sign it, and then store the audit.
- Aadhaar authentication PID block should not be audited.

Reporting and analytics modules can be built and offered as a value added service to subscribers of e-Sign service. **Providers must ensure reporting/analytics sub-system contain no resident PII via proper anonymization**. No individual people level analytics should be performed to ensure privacy is maintained.

e-Sign provider, based on their pricing plans and contract structure with their subscribers, can use transaction analytics for billing purposes. CCA may regulate the pricing via some "cap" (maximum price), but, should allow providers to offer flexible pricing and value added services to their subscribers. Market forces should determine the winner in terms of quality and affordability of e-SIgn service. Having multiple e-Sign providers eliminates monopoly.